ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ
INFORMATION TECHNOLOGY, COMPUTER SCIENCE, AND MANAGEMENT



УДК 519.72; 519.876.5 https://doi.org/10.23947/2687-1653-2021-21-1-96-104

О модификации декодера bit-flipping кодов с низкой плотностью проверок на четность



С. С. Гурский, Н. С. Могилевская
ФГАОУ ВО «Южный федеральный университет» (г. Ростов-на-Дону, Российская Федерация)

Введение. Во всех видах цифровой связи применяются методы помехоустойчивого кодирования. Во многих стандартах цифровой связи, например вай-фай (англ. Wi-Fi) и 5G, используются коды с низкой плотностью проверок на четность. Эти коды популярны потому, что для них возможно построение кодеров и декодеров с невысокой вычислительной сложностью. Цель настоящей работы — повышение корректирующей способности известного битфлиппинг-декодера (англ. bit-flipping, BF) LDPC-кодов. Для этого строится модификация декодера, позволяющая динамически управлять одним из его основных параметров, выбор которого существенно влияет на качество декодирования.

Материалы и методы. Рассмотрен известный декодер bit-flipping двоичных LDPC-кодов. Некоторые его параметры не имеют жесткой связи с параметрами кода. С помощью имитационного моделирования исследована зависимость качества декодирования от выбора выходных параметров декодера bit-flipping. Показано, что на результаты декодирования в этом случае существенно влияет входной параметр декодера — порог T. Разработана модификация BF-декодера двоичных LDPC-кодов, в которой предлагается задавать порог динамически во время выполнения алгоритма в зависимости от степени повреждения кодового слова ошибками. Проведен сравнительный анализ корректирующей способности декодеров методом имитационного моделирования.

Результаты исследования. Сформулирована и доказана лемма о максимальном значении порога T декодера. Найдены верхние оценки для количества операций оригинального и модифицированного декодеров. Построена имитационная модель, реализующая цифровой помехоустойчивый канал связи. В модели исходные данные кодируются заданным LDPC-кодом, зашумляются аддитивными равномерно распределенными ошибками, а затем поочередно декодируются алгоритмом bit-flipping с различными параметрами порога T и модифицированным декодером. По входным и выходным данным оценивается корректирующая способность использованных декодеров. Эксперименты показали, что в диапазоне реального уровня ошибок корректирующая способность модифицированного декодера выше, чем у оригинального, вне зависимости от выбора его параметров.

Обсуждение и заключения. Доказанная в работе лемма устанавливает верхнюю границу значения порога в оригинальном декодере, что облегчает его настройку. По сравнению с оригинальным декодером разработанная модификация способна лучше исправлять ошибки. При этом сложность модификации увеличена незначительно по сравнению с оригинальным алгоритмом. Отмечено, что качество декодирования модифицированным декодером растет при увеличении длины кода и уменьшении количества циклов в графе Таннера, соответствующего проверочной матрице кода.

Ключевые слова: LDPC-коды, корректирующая способность декодера, динамический порог, двоичный симметричный канал, экспериментальное исследование.

Для цитирования: Гурский, С. С. О модификации декодера bit-flipping кодов с низкой плотностью проверок на четность / С. С. Гурский, Н. С. Могилевская // Advanced Engineering Research. — 2021. — Т. 21, № 1. — С. 96–104. https://doi.org/10.23947/2687-1653-2021-21-1-96-104



On the modification of bit-flipping decoder of LDPC-codes

S. S. Gurskiy, N. S. Mogilevskaya
Southern Federal University (Rostov-on-Don, Russian Federation)

Introduction. In all types of digital communication, error control coding techniques are used. Many digital communication standards, such as Wi-Fi and 5G, use low density parity check (LDPC) codes. These codes are popular because they provide building encoders and decoders with low computational complexity. This work objective is to increase the error correcting capability of the well-known bit-flipping decoder (BF) of LDPC-codes. For this purpose, a modification of the decoder is built, which enables to dynamically control one of its main parameters whose choice affects significantly the quality of decoding.
Materials and Methods. The well-known bit-flipping decoder of binary LDPC-codes is considered. This decoder has several parameters that are not rigidly bound with the code parameters. The dependence of the decoding quality on the selection of the output parameters of the bit-flipping decoder was investigated through simulation modeling. It is shown that the decoding results in this case are significantly affected by the input parameter of the decoder — threshold *T*. A modification of the BF-decoder of binary LDPC-codes has been developed, in which it is proposed to set the threshold dynamically during the execution of the algorithm depending on the error rate. A comparative analysis of the error-correcting capability of decoders is carried out by the simulation modeling method.
Results. A lemma on the maximum value of the decoder threshold *T* is formulated and proved. Upper bounds for the number of operations are found for the original and modified decoders. A simulation model that implements a digital noise-immune communication channel has been built. In the model, the initial data is encoded with a given LDPC-code, then it is made noisy by additive uniformly distributed errors, and thereafter, it is decoded in turn by the bit-flipping algorithm with different threshold *T* parameters, as well as by a modified decoder. Based on the input and output data, the correction capacity of the decoders used is estimated. Experiments have shown that the error-correcting capability of the modified decoder in the range of the real error rate is higher than that of the original decoder, regardless of the selection of its parameters.
Discussion and Conclusions. The lemma, proved in the paper, sets the upper bound on the threshold value in the original decoder, which simplifies its adjustment. The developed modification of the decoder has a better error-correcting capability compared to the original decoder. Nevertheless, the complexity of the modification is slightly increased compared to the original algorithm. It has been pointed out that the decoding quality of a modified decoder develops with a decrease in the number of cycles in the Tanner graph and an increase in the length of the code.

***Keywords**:* LDPC-codes, error-correcting capability, dynamic threshold, binary symmetric channel, experimental research.

For citation: S. S. Gurskiy, N. S. Mogilevskaya. On the modification of bit-flipping decoder of LDPC-codes. Advanced Engineering Research, 2021, vol. 21, no. 1, p. 96–104. https://doi.org/10.23947/2687-1653-2021-21-1-96-104

Введение. В 1963 году в работе [1] Р. Галлагер впервые описал класс линейных блочных кодов, проверочная матрица которых содержит малое количество ненулевых элементов. Такие коды принято называть кодами с низкой плотностью проверок на четность или LDPC-кодами (от англ. low-density parity check codes). Для них возможно построение кодеров и декодеров с невысокой вычислительной сложностью. Таким образом, при использовании LDPC-кодов скорость передачи данных существенно не ограничивается. Многие современные работы посвящены LDPC-кодам и их декодерам [2–5]. LDPC-коды активно используются в разных стандартах цифровой связи, например вай-фай (англ. Wi-Fi), 5G и оптической связи [6, 7]. Однако, несмотря на популярность этих кодов, некоторые связанные с ними задачи требуют исследования и решения. Одна из них — построение новых и улучшение существующих декодеров.

Цель данной работы — повышение корректирующей способности известного декодера bit-flipping LDPC-кодов (далее BF-декодер). Для этого строится модификация декодера, позволяющая динамически управлять одним из его основных параметров, выбор которого существенно влияет на качество декодирования.

Материалы и методы. Основными параметрами двоичных LDPC-кодов являются длина N, размерность K и минимальное расстояние кода d. Информационные слова $[N, K, d]$-кода C — это векторы $\bar{m} = (m_1, m_2, \dots, m_K) \in F_2^K$, где F_2 — поле Галуа мощности 2, а кодовые слова — векторы $\bar{c} = (c_1, c_2, \dots, c_N) \in F_2^N$ [8]. Удобно задавать LDPC-коды проверочной $(N - K) \times N$ матрицей H. Большее количество ее элементов — нулевые [1], поэтому удобнее хранить ее не целиком, а запоминая только позиции ненулевых элементов по строкам.

Различают регулярные [9] и нерегулярные [10] LDPC-коды. В регулярных кодах все строки и столбцы проверочных матриц содержат фиксированное количество единичных элементов (k и j соответственно), иначе

код называют нерегулярным. Для удобства проверочные матрицы регулярных LDPC-кодов будем называть регулярными матрицами, а нерегулярных LDPC-кодов — нерегулярными.

Регулярные LDPC-коды обладают рядом преимуществ: легко оцениваемые параметры кода, удобство хранения матриц, невысокая вычислительная сложность алгоритмов кодирования и декодирования и пр. Кроме этого, декодеры регулярных кодов исправляют ошибки равномерно, в отличие от нерегулярных, которые исправляют ошибки в некоторых частях кодового слова хуже, чем в других. Однако задача генерации регулярных матриц с заданными свойствами является сложной, часто для ее решения используются методы перебора.

Для обсуждения свойств матрицы H удобно использовать соответствующий ей граф Таннера $G = (V, E)$, где E — множество ребер, а $V = S \cup R$ — множество вершин, S — множество строк матрицы H, а R — множество ее столбцов [11]. Каждый ненулевой элемент H, стоящий в i-й строке и j-м столбце, задает ребро, соединяющее -ю вершину множества S и j-ю вершину множества R. На рис. 1 представлен пример регулярной проверочной матрицы 3×6 с параметрами $k = 4$ и $j = 2$ и соответствующий ей граф Таннера.

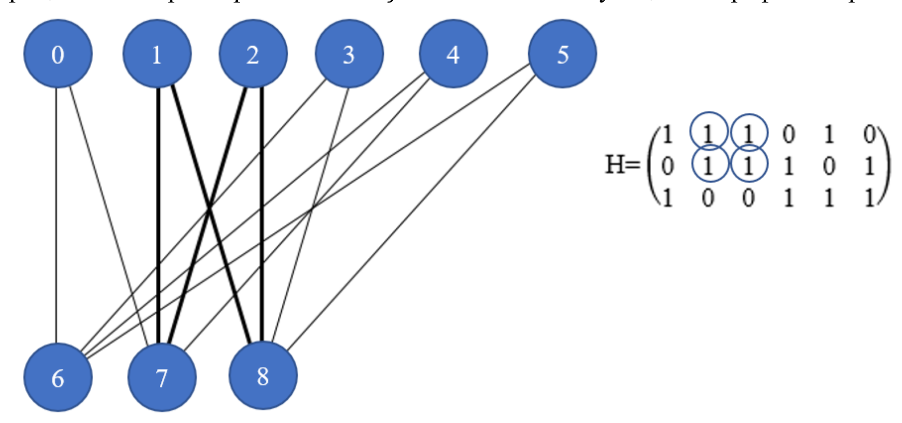


Рис. 1. Цикл в графе Таннера и в проверочной матрице

Верхний ряд вершин графа соответствует столбцам матрицы H, а нижний ряд связан со строками H. Важная характеристика проверочной матрицы H LDPC-кода — наличие и тип циклов в соответствующем ей графе Таннера. Цикл — это такая последовательность смежных вершин графа, в которой первая и последняя вершины совпадают. Длина этой последовательности называется длиной цикла. Минимальная длина цикла в графе называется обхватом. Если граф не содержит циклов, его обхват полагают бесконечным. Пример цикла длины 4 выделен жирными линиями на графе (рис. 1).

Возможности по исправлению ошибок зависят не только от основных параметров LDPC-кодов, но и от структуры проверочной матрицы H. С одной стороны, наличие циклов небольших длин (таких как 4 и 6) заметно ухудшает корректирующую способность декодера [12]. С другой стороны, код, которому соответствует граф Таннера без циклов, не исправляет ошибок, т. к. его минимальное кодовое расстояние равно 2. Таким образом, задача построения проверочных матриц регулярных LDPC-кодов является многопараметрической. При ее решении необходимо следить за основными параметрами кода, а также за циклами в графе Таннера, соответствующем проверочной матрице.

Рассмотрим в удобном виде известный BF-декодер LDPC-кода C [13].

Вход: LDPC-код C с параметрами $[N, K, d]$, заданный проверочной матрицей

$$H = \begin{pmatrix} h_{11} & h_{12} & \dots & h_{1N} \\ h_{21} & h_{22} & \dots & h_{2N} \\ \dots & \dots & \ddots & \dots \\ h_{(N-K)1} & h_{(N-K)2} & \dots & h_{(N-K)N} \end{pmatrix}. \quad (1)$$

Вектор $\bar{c}' = \bar{c} + \bar{e}$, $\bar{c} \in C(\subset F_2^N)$, $\bar{e}(\in F_2^N)$ — вектор ошибок; p — количество итераций алгоритма; T — пороговое значение.

Выход: кодовый вектор $\bar{c} \in C(\subset F_2^N)$.

Шаг 1. Положим счетчик r равным нулю.

Шаг 2. Вычислим синдром $\bar{s} = \bar{c}' H^T$. Если $\bar{s} = \bar{0}$ или $r = p$, то переходим на шаг 5.

Шаг 3. Выделим из вектора $\bar{s} = (s_1, s_2, \dots, s_{N-K})$ единичные координаты, т. е. $s_i = 1$, $i = \overline{1,(N-K)}$. Составим множество $L = \{i | s_i = 1\}$. Вычислим $\bar{h}' = (h'_1, h'_2, \dots, h'_N)$, где

$$h'_l = \sum_{i \in L} h_{il}. \quad (2)$$

Величины h_{il}, $l = 1, \ldots, N$ следует полагать неотрицательными целыми числами. Таким образом, $\bar{h}' \in \mathbb{N}_0^N$, где $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

Шаг 4. В векторе $\bar{h}' = (h'_1, h'_2, \ldots, h'_N)$ находим все элементы $h'_i > T$. Среди них выбираем случайный h'_l и инвертируем бит c'_l вектора $\bar{c}$. Добавляем к счетчику r единицу и переходим на шаг 2.

Шаг 5. $\bar{c} \coloneqq \bar{c}'$.

Исследования, проведенные в рамках данной работы, позволяют сделать ряд замечаний по BF-декодеру.

Замечание 1. Входной параметр p задает максимальное количество итераций алгоритма со 2-го по 4-й шаги, но декодер может восстановить кодовое слово за меньшее число итераций.

Замечание 2. При выборе параметра T нужно руководствоваться следующими соображениями. Если известен параметр d используемого $[N, K, d]$-кода C, то по нему можно вычислить t — число гарантированно исправляемых ошибок, и тогда количество итераций декодера ограничивается этим значением:

$$p = t = \left\lfloor \frac{d-1}{2} \right\rfloor. \quad (3)$$

Здесь $\lfloor x \rfloor$ — округление числа x до меньшего целого. Если параметр d неизвестен, то его можно оценить с помощью границы Синглтона [5]

$$d \leq N - K + 1$$

и, используя (3), получить

$$p = \left\lfloor \frac{N-K}{2} \right\rfloor.$$

Замечание 3. Структура декодера такова, что восстановление корректного кодового слова не гарантируется, даже если в зашумленном слове $\bar{c}' = \bar{c} + \bar{e}$ возникло не более t ошибок (3).

Замечание 4. В литературе для регулярных проверочных матриц в BF-декодере рекомендуется выбирать порог T зависящим от веса j столбца матрицы H, а именно $T = \frac{j}{2}$. Для нерегулярных матриц такие рекомендации в литературе не приведены. Корректирующую способность BF-декодера может ухудшить неудачный выбор порога T. При его большом значении на шаге 4 декодера в векторе $\bar{h}'$ может не найтись координаты, превосходящей порог T, следовательно, не будут исправлены ошибочные биты. При выборе малого значения T на шаге 4 BF-декодера в векторе $\bar{h}'$ может появиться несколько координат, значение которых превышает порог. Среди них могут быть и координаты, не содержащие ошибку. Таким образом, выбор параметра T может в значительной мере повлиять на качество декодирования.

Результаты исследования. Сформулируем и докажем лемму о максимально возможном значении порога T. Затем модифицируем BF-декодер таким образом, чтобы порог устанавливался в процессе декодирования динамически, и проведем сравнительный анализ оригинального и модифицированного алгоритмов декодирования.

Лемма. Пусть двоичный $[N, K, d]$-код C задан с помощью проверочной матрицы H, имеющей фиксированное количество j единичных элементов в каждом столбце. Тогда максимальное значение порога T для BF-декодера такого LDPC-кода C не может быть больше

$$T = j - 1. \quad (4)$$

Доказательство. Пусть из канала передачи получен вектор $\bar{c}' = \bar{c} + \bar{e}$, где $\bar{c} \in C$ — верное кодовое слово, $\bar{e} \in F_2^N$ — вектор ошибок с весом Хэмминга $w(\bar{e})$. Если $w(\bar{e}) = 0$, то на шаге 2 вектор-синдром $\bar{s} = \bar{0}$. Следовательно, алгоритм перейдет на шаг 5 и вернет $\bar{c}'$ в качестве ответа. В этом случае значение порога не используется. Если $w(\bar{e}) > 0$, то из регулярности H вытекает справедливость неравенства $h'_l \leq j$, где h'_l — элементы вектора $\bar{h}'$. Инвертирование бит c_l вектора $\bar{c}'$ происходит в алгоритме, только если $h'_l > T$. Следовательно,

$$T < h'_l \leq j.$$

Таким образом, формула (4) верна.

Внесем в BF-декодер изменения, которые позволят определять величину порога динамически, в зависимости от степени повреждения кодового вектора в канале передачи.

Вход: $[N, K, d]$-код C, заданный приведенной выше проверочной матрицей (1). Вектор $\bar{c}' = \bar{c} + \bar{e}$, где $\bar{c} \in C(\subset F_2^N), \bar{e}(\in F_2^N)$ — вектор ошибок; p — количество итераций алгоритма; T — некоторое пороговое значение, выбранное заранее.

Выход: кодовый вектор $\bar{c} \in C(\subset F_2^N)$.

Шаг 1. Положим счетчик r равным нулю.

Шаг 2. Вычислим синдром $\bar{s} = \bar{c}' H^T$. Если $\bar{s} = (0, \dots, 0)$ или $r = p$, то переходим на шаг 7.

Шаг 3. Выделим из вектора $\bar{s} = (s_1, s_2, \dots, s_{N-K})$ единичные координаты, т. е. $s_i = 1$, $i = \overline{1, (N-K)}$. Составим множество $L = \{i | s_i = 1\}$. Вычислим $\bar{h}' = (h'_1, h'_2, \dots, h'_N)$, где h'_l такой же, как и в оригинальном декодере (2). При суммировании величины h_{il} $l = 1, \dots, N$, следует полагать неотрицательными целыми числами. Таким образом, $\bar{h}' \in \mathbb{N}_0^N$, где $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

Шаг 4. Инициализируем значение порога $T \coloneqq \max(h'_l)_{l=1,\dots,N} - 1$.

Шаг 5. Если $T \geq 0$

Выберем произвольный элемент h'_q вектора $\bar{h}'$ — такой, что $h'_q > T$.

Инвертируем бит c'_q.

Шаг 6. Добавим к счетчику r единицу и перейдем на шаг 2.

Шаг 7. $\bar{c} \coloneqq \bar{c}'$.

Замечание 5. Модифицированный алгоритм в целом выполняет меньше итераций, чем BF-декодер, т. к. на шаге 4 порог выбирается динамически. Следовательно, декодер не выполняет бесполезные итерации, на которых не изменяются биты вектора $\bar{c}'$. Значение порога в модифицированном декодере зависит от числа ошибок, повредивших кодовое слово, и сразу устанавливается таким, что в зашумленное кодовое слово $\bar{c}'$ гарантированно вносятся изменения.

Оценим сверху количество операций сложения, сравнения и присваивания в обоих декодерах. В оригинальном BF-декодере $[N, K, d]$-кода C производится $p(kK + (N-K)N + 1)$ операций сложения, $p(3N - 2K + 2)$ операций сравнения и $p\big((N-K)(k+1) + 2N + 3\big) + 1$ операций присваивания. В BF-декодере с динамическим порогом — $p(kK + (N-K)N + 3)$ операций сложения, $p(5N - 2K + 3)$ операций сравнения и $p\big((N-K)(k+1) + 2N + 4\big) + 1$ операций присваивания. Здесь p — параметр декодера, устанавливающий максимальное количество операций, k — вес строк проверочной матрицы кода. Заметим, что при реализации алгоритма фактически не используются операции умножения и деления, т. к. на втором шаге для вычисления синдрома $\bar{s}$ удобно использовать операции сложения вместо умножения. Напомним, что матрица H обладает разреженной структурой, и ее строки удобно хранить в виде списка номеров ненулевых элементов. Следовательно, вместо умножения вектора $\bar{c}'$ на матрицу H необходимо суммировать координаты вектора $\bar{c}'$, номера которых совпадают с номерами ненулевых элементов в соответствующей строке матрицы H.

В сравнении с оригинальным алгоритмом модифицированный BF-декодер выполняет больше операций, но не значительно: число операций сравнения увеличилось на $p(2N + 1)$, присваивания — на p, сложения — на $2p$.

Для сравнительного исследования корректирующей способности оригинального и модифицированного алгоритмов декодирования создано программное средство, реализующее имитационную модель двоичного симметричного идеально синхронизированного помехоустойчивого канала связи согласно [14–16]. Для обеспечения помехоустойчивости в модели использованы LDPC-коды и BF-декодеры (оригинальный и с динамическим порогом). Ошибки в канале моделировались независимыми и равномерно распределенными.

В экспериментах использованы специально найденные проверочные матрицы, задающие LDPC-коды. Опишем основные параметры этих матриц, используя стандартные обозначения основных параметров кода, а также: j и k — вес каждого столбца и вес каждой строки проверочной матрицы соответственно; ω_4, ω_6 — 4 и 6 циклов в графе Таннера, соответствующем проверочной матрице.

Регулярная матрица H_1: $N = 20$, $K = 5$, $j = 3$, $k = 4$, $d = 6$, $\omega_4 = 0$, $\omega_6 = 41$.
Регулярная матрица H_2: $N = 28$, $K = 7$, $j = 3$, $k = 4$, $d = 6$, $\omega_4 = 0$, $\omega_6 = 42$.
Регулярная матрица H_3: $N = 28$, $K = 7$, $j = 3$, $k = 4$, $d = 6$, $\omega_4 = 0$, $\omega_6 = 29$.
Нерегулярная матрица H_4: $N = 32$, $K = 5$, $j = 3$, $d = 12$, $\omega_4 = 0$, $\omega_6 = 0$.

С использованием этих матриц были построены кодеки LDPC-кодов и проведены имитационные эксперименты. На рис. 2–5 представлены графики зависимости корректирующей способности построенных

кодеков LDPC-кодов от вероятности ошибки в канале. Обоснование выбора значений порога $T = 1$ и $T = 2$ в BF-декодере см. в замечаниях 3, 4 и лемме.

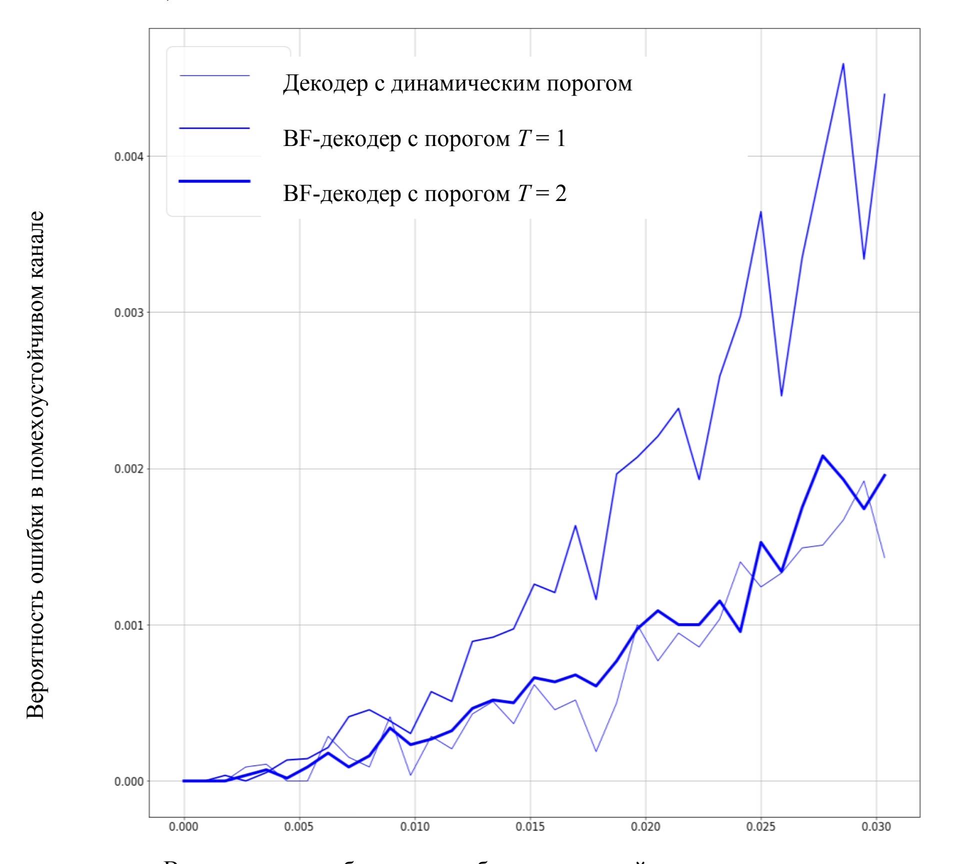


Рис. 2. График корректирующей способности декодеровдля LDPC-кодов, заданных матрицей H_2



Рис. 3. График корректирующей способности декодеров для LDPC-кодов, заданных матрицей H_3



Рис. 4. График корректирующей способности декодеров для LDPC-кодов, заданных матрицей H_4

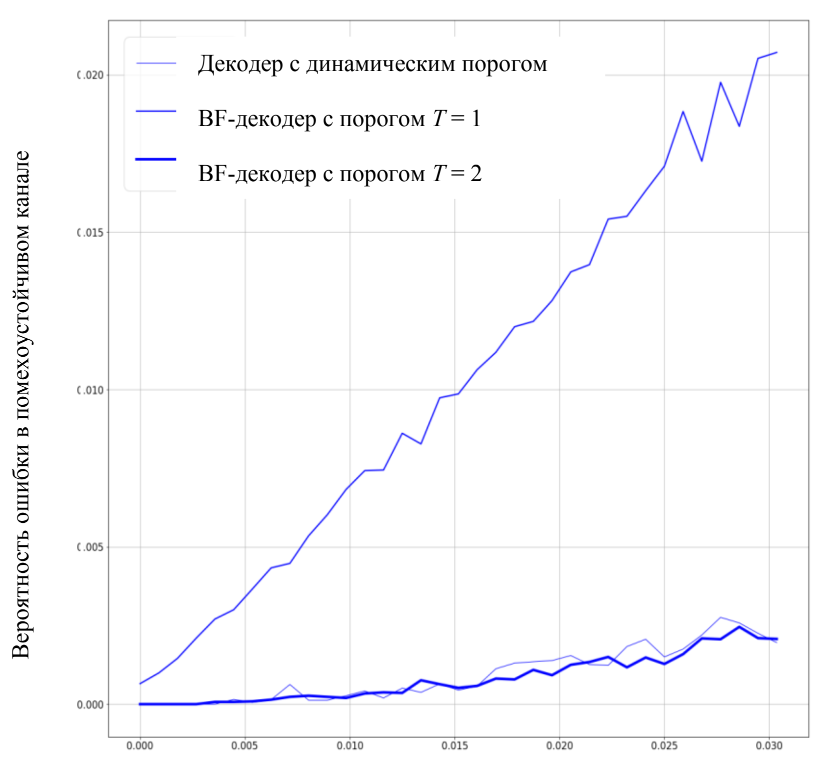


Рис. 5. График корректирующей способности декодеров для LDPC-кодов, заданных матрицей H_1

В диапазоне реального уровня ошибок [8, 13, 14] на рис. 2–4 можно наблюдать, что BF-декодер при значении порога $T = 2$ показывает лучшие результаты, чем при $T = 1$, а модифицированный BF-декодер обладает лучшей корректирующей способностью по сравнению с оригинальным.

Декодеры демонстрируют схожую эффективность при малых значениях длины кода, однако при ее увеличении модифицированный декодер показывает лучшие результаты. Так, при вероятности ошибки в

непомехоустойчивом канале 0,05 различие в вероятности ошибки в помехоустойчивом канале при использовании BF-декодера с порогом $T = 2$ и $T = 1$ составляет от 0,005 до 0,03 в пользу использования большего значения порога. Если же задействовать BF-декодер с порогом $T = 2$ и модифицированный декодер, это различие колеблется в зависимости от LDPC-кода в интервале от 0,001 до 0,003. При вероятности ошибки в непомехоустойчивом канале 0,1 вероятность ошибки в помехоустойчивом канале при использовании BF-декодера с порогом $T = 2$ меньше, чем с порогом $T = 1$, на величину от 0,001 до 0,02. При использовании BF-декодера с порогом $T = 2$ и модифицированного декодера это различие колеблется в зависимости от LDPC-кода в интервале от 0,002 до 0,01.

Оба декодера чувствительны к количеству циклов в графе Таннера, соответствующему проверочной матрице LDPC-кода. Чем больше отношение количества циклов к общему количеству элементов в матрице, тем хуже исправляет ошибки любой BF-декодер. При проведении экспериментов было интересно выяснить, можно ли так увеличить количество циклов в матрице, что модифицированный декодер покажет худшие результаты по сравнению с BF-декодером. Опытным путем была найдена такая матрица — H_1, содержащая 41 цикл длины 6. Результаты исследования корректирующей способности декодеров для этой матрицы показаны на рис. 5. Заметим, однако, что матрица H_2 содержит еще больше циклов длины 6, а именно 42. Принципиальное отличие матриц H_1 и H_2 — в плотности единиц:

— в H_1 — 60 единичных элементов на 300 элементов матрицы,

— в H_2 — 84 единицы на 588 элементов матрицы.

Напомним, что особенностью LDPC-кодов является разреженная структура проверочной матрицы, поэтому H_2 более типична для LDPC-кодов.

Обсуждение и заключения. В работе рассмотрен декодер bit-flipping двоичных LDPC-кодов. Даны рекомендации о выборе таких входных параметров декодера, как порог и количество итераций алгоритма. Сформулирована и доказана лемма о максимальном значении порога декодера. Разработана модификация BF-декодера двоичных LDPC-кодов, в которой предлагается задавать порог динамически во время выполнения алгоритма в зависимости от полученного синдрома. Для оригинального и модифицированного декодеров найдены верхние оценки количества операций. Эти оценки показывают, что модификация усложняет декодер незначительно. Проведенные имитационные эксперименты демонстрируют лучшую корректирующую способность модифицированного декодера по отношению к оригинальному. Эксперименты также показали зависимость качества декодирования от степени разреженности матрицы и количества циклов длины 6 в графе Таннера, соответствующего проверочной матрице LDPC-кода. Таким образом, возникает задача построения проверочных матриц с малым количеством коротких циклов, что является предметом дальнейших исследований.

Библиографический список

1. Gallager, R. Low-density parity-check codes / R. Gallager // IRE Transactions on information theory. — 1962. — Vol. 8, no. 1. — P. 21–28.

2. Milicevic, M. Quasi-cyclic multi-edge LDPC codes for long-distance quantum cryptography / M. Milicevic, Ch. Feng, L. M. Zhang [et al.] // NPJ Quantum Information. — 2018. — No. 4 (1). — P. 1–9. DOI : 10.1038/s41534-018-0070-6

3. Chen, P. Rate-Adaptive Protograph LDPC Codes for Multi-Level-Cell NAND Flash Memory / P. Chen, K. Cai, S. Zheng // IEEE Communications Letters. — 2018. Vol. 22, iss. 6. — P. 1112–1115. DOI : 10.1109/LCOMM.2018.2814985

4. Baldi, M. A Post-quantum Key Encapsulation Mechanism Based on QC-LDPC Codes. Post-Quantum Cryptography / M. Baldi, A. Barenghi, F. Chiaraluce [et al.] // PQCrypto 2018 : Lecture Notes in Computer Science. — Cham : Springer, 2018. — Vol. 10786. — P. 3–24. DOI : 10.1007/978-3-319-79063-3_1

5. Maity, R. K. Robust Gradient Descent via Moment Encoding and LDPC Codes / R. K. Maity, R. A. Singh, A. Mazumdar // In: Proc. IEEE International Symposium on Information Theory (ISIT). — Paris : IEEE, 2019. — P. 2734–2738. DOI : 10.1109/ISIT.2019.8849514

6. Li H. Algebra-Assisted Construction of Quasi-Cyclic LDPC Codes for 5G New Radio / Li H, Bai B, Mu X [et al.] // IEEE Access. — 2018. — Vol. 6. — P. 50229–50244. DOI : 10.1109/ACCESS.2018.2868963

7. Cai, Z. Efficient encoding of IEEE 802.11n LDPC codes / Z. Cai, J. Hao, P. H. Tan [et al.] // Electronics Letters. — 2006. — Vol. 42, iss 25. — P. 1471–1472. DOI : 10.1049/el:20063126

8. Колесник, В. Д. Кодирование при передаче и хранении информации / В. Д. Колесник. — Москва : Высшая школа, 2009. — 550 с.

9. Tong Zhang. Joint(3,k)-regular LDPC code and decoder/encoder design // Tong Zhang, K. K. Parhi // IEEE Transactions on Signal Processing. — 2004. — Vol. 52, iss. 4. — P. 1065–1079. DOI : 10.1109/TSP.2004.823508

10. Yang, M. Design of efficiently encodable moderate-length high-rate irregular LDPC codes / M. Yang, W. E. Ryan, Yan Li // IEEE Transactions on Communications. — 2004. — Vol. 52, iss. 4. — P. 564–571.

11. Malema, G. A. Low-Density Parity-Check Codes: Construction and Implementation / G. A. Malema. — University of Adelaide, 2007. — 160 p. URL : https://digital.library.adelaide.edu.au/dspace/bitstream/2440/45525/8/02whole.pdf (accessed : 07.06.2020).

12. Etzion, T. Which codes have cycle-free Tanner graphs? / T. Etzion, A. Trachtenberg, A. Vardy // IEEE Transactions on Information Theory. — 2006. — Vol. 52, iss. 9. — P. 4219–4223. DOI: 10.1109/TIT.2006.880060

13. Морелос-Сарагоса, Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение / Р. Морелос-Сарагоса. — Москва : Техносфера, 2006. — С. 259–262.

14. Деундяк, В. М. Методы оценки применимости помехоустойчивого кодирования в каналах связи / В. М. Деундяк, Н. С. Могилевская. — Ростов-на-Дону : Изд-во ДГТУ, 2007. — 85 с.

15. Деундяк, В. М. Решение задачи подбора модели источника ошибок в ИС ОПСАПК / В. М. Деундяк, М. А. Жданова, Н. С. Могилевская // Вестник Донского государственного технического университета. — 2017. — № 17 (4). — С. 107–115. DOI : 10.23947/1992-5980-2017-17-4-107-115

16. Деундяк, В. М. Имитационная модель цифрового канала передачи данных и алгебраические методы помехоустойчивого кодирования / В. М. Деундяк, Н. С. Могилевская // Вестник Донского государственного технического университета. — 2001. — № 1 (1). — С. 98–104.

Сдана в редакцию 26.10.2020
Принята к публикации 25.01.2021

Об авторах:

Гурский Семен Сергеевич, аспирант кафедры «Алгебра и дискретная математика» ФГАОУ ВО «Южный Федеральный университет (344090, РФ, г. Ростов-на-Дону, ул. Мильчакова, 8а), ORCID: https://orcid.org/0000-0002-4738-2363, nor-ber@list.ru.

Могилевская Надежда Сергеевна, доцент кафедры «Алгебра и дискретная математика» ФГАОУ ВО «Южный Федеральный университет (344090, РФ, г. Ростов-на-Дону, ул. Мильчакова, 8а), кандидат технических наук, доцент, ORCID: http://orcid.org/0000-0003-1357-5869, nadezhda.mogilevskaia@yandex.ru.

Заявленный вклад соавторов:

С. С. Гурский — модификация декодера bit-flipping, программная реализация моделей каналов, проведение вычислительных экспериментов, подготовка текста. Н. С. Могилевская — научное руководство, постановка задачи, анализ результатов исследований, доработка текста, формулирование выводов.

Все авторы прочитали и одобрили окончательный вариант рукописи.